UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The Cellular Telephone Serviced by T-Mobile, as More Fully Described in Attachment A.

Case No. 25 MJ 119

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 371 and 2313	(conspiracy to violate the laws of the United States, and sale, receipt, possession, or concealment of stolen vehicles)

The application is based on these facts:

See the attached affidavit.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Shane Hoffmann, Special Agent (FBI)
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 06/24/2025

Judge's signature

City and state: Milwaukee, Wisconsin

William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Shane Hoffmann, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A) for information about the historical and prospective location of a cellular device ("Target Cell Phone 1" or "TCP-1"). The service provider for TCP-1 is T-Mobile (the "Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. TCP-1 is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from TCP-1.

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since September 2015. I am currently assigned to the Milwaukee Division – Madison Resident Agency. Since becoming a Special Agent, I have received specialized training in conducting criminal investigations, and my responsibilities include conducting investigations of alleged criminal violations of federal statutes and laws and apprehending fugitives. I have

experience and have been trained in the investigation of an array of federal criminal violations. Through investigations and training I am familiar with how cell phones and other technical data can be used to commit federal offenses, and I have authored numerous affidavits relating to cellular devices, cell site location information, and other technical data.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that TASHAWN BROWN-SMITH has violated 18 U.S.C. § 371 (conspiracy to violate the laws of the United States) and18 U.S.C. § 2313 (sale, receipt, possession, or concealment of stolen vehicles). TASHAWN BROWN-SMITH was charged with these crimes on June 24, 2025 and is the subject of an arrest warrant issued that date. There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting TASHAWN BROWN-SMITH, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

5. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

6. The United States, including Federal Bureau of Investigation, is conducting a criminal investigation of DIAUNTE D. SHIELDS, GEOFFREY HARVEY, WILLIE BULLARD, LASHAWN DAVIS, JR., BRANDON MULLINS, NAKIYA WRIGHT, CASHA GRIFFIN, BRIANNA SHIELDS, GERRICA BAKER, DEON BROOKS, CHANDOR SMITH, TASHAWN BROWN-SMITH, DEQUAS CRAWFORD-HIGGS, JA LEAN LITTLE, VASHAWN MILTON, DEAMONTE LEE, GLENN LARSEN, KENNETH KILSON, CHAZ HOLIFIELD, MELIEK McCLARN, TASHAY NORTHERN, ESTEBAN CARDENAS,

ENRICO WILLIAMS, and unidentified subjects regarding possible violations of 18 U.S.C. §§ 371, 511, 514, 1001, 1028A, 1956, 2312, 2313, 2321, and 2(a); 21 U.S.C. §§ 841(a)(1), 841(b)(1)(A), 841(b)(1)(B), and 846.

7. On June 13, 2025, U.S. Magistrate Judge William E. Duffin of the Eastern District of Wisconsin authorized a pen register and trap and trace for information pertaining to BROWN-SMITH's known Facebook account, the display name for which is "Srt Ball Out," a reference to Dodge and Jeep's "Street and Racing Technology" (SRT), and the unique user name for which is "tashawn.smith.7". The Facebook subscriber information shows that multiple phone numbers that investigators have connected to BROWN-SMITH are linked to his Facebook account including phone number 779-240-6814. Phone subscriber information shows that 779-240-6814 was subscribed to Tashawn Smith, 1316 Indian Trail, Kanakee (sic), Illinois. Multiple images on the publicly viewable account are consistent with known images of BROWN-SMITH.

8. From June 14, 2025 through June 19, 2025, data received from Facebook via Meta Platforms, Inc. ("Meta") has shown that BROWN-SMITH has approximately 200 log-in events using IP addresses associated with T-Mobile including the following:

Event Time (UTC)	IP Address
2025-06-17 21:27:09	**2607:fb90:9b0f:c247:d4d5:2e2f:ff82:e6b3**
2025-06-18 18:37:21	**2607:fb90:a273:ce5a:6803:b74e:e78b:51ff**
2025-06-19 09:40:32	**2607:fb91:2285:25f:9557:8247:d5ff:2e7f**

9. Therefore, with this warrant I seek subscriber information, along with historical location information dating back to June 1, 2025 to determine BROWN-SMITH's historical patterns of life and movement and prospective location information to identify his location at given

times in order to execute the pending arrest warrant, from T-Mobile for the phone number associated with the IP addresses that have been used to login into BROWN-SMITH's Facebook account around the timeframes referenced above (TCP-1). Law enforcement will use this information to locate BROWN-SMITH with more precision and arrest BROWN-SMITH pursuant to the federal arrest warrant referenced above.

TECHNICAL BACKGROUND

10. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

Cell-Site Data

11. Based on my training and experience, I know that the Service Provider can collect cell-site data on a prospective basis about TCP-1. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the

cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

E-911 Phase II / GPS Location Data

12. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training and experience, I know that the Service Provider can collect E-911 Phase II data about the location of TCP-1, including by initiating a signal to determine the location of TCP-1 on the Service Provider's network or with such other reference points as may be reasonably available.

Pen-Trap Data

13. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the

embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers—as transmitted from a cellular device to a cellular antenna or tower—can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

Subscriber Information

14. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify TCP-1's user or users and may assist in the identification of co-conspirators.

AUTHORIZATION REQUEST

15. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

16. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

17. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of TCP-1 on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

18. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice for 30 days. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of TCP-1 would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

19. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate TCP-1 outside of daytime hours.

ATTACHMENT A

Property to Be Searched

Matter No. 2022R00208

1. Records and information associated with the electronic device ("Target Cell Phone 1" or "TCP-1") that accessed the Internet using any of the IP addresses below around the associated dates and times:

Event Time (UTC)	IP Address
2025-06-17 21:27:09	**2607:fb90:9b0f:c247:d4d5:2e2f:ff82:e6b3**
2025-06-18 18:37:21	**2607:fb90:a273:ce5a:6803:b74e:e78b:51ff**
2025-06-19 09:40:32	**2607:fb91:2285:25f:9557:8247:d5ff:2e7f**

Such information being in the custody or control of T-Mobile (the "Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

2. Target Cell Phone 1.

ATTACHMENT B

Matter No. 2022R00208

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the accounts listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with TCP-1 for the time period from June 1, 2025, to present:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International

Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address);

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records; and

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by TCP-1, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses);

(B) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received); and

(C) all historical Timing Advance Data (TrueCall).

b. Information associated with each communication to and from TCP-1 for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication;

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which TCP-1 or will connect at the beginning and end of each communication; and

v. All precision location and/or GPS information associated with the account, including Timing Advance Data (TrueCall).

The Court has also issued an order pursuant to 18 U.S.C. § 3123, dated today, for such information associated with TCP-1.

c. Information about the location of TCP-1 for a period of 30 days, during all times of day and night. "Information about the location of TCP-1" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of TCP-1 on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that will assist in arresting TASHAWN BROWN-SMITH, who was charged with violating 18 U.S.C. §§ 371 and 2313 on June 24, 2025, is the subject of an arrest warrant issued on June 24, 2025, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.